

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

Robert C. Schubert (S.B.N. 62684)
(rschubert@sjk.law)
Dustin L. Schubert (S.B.N. 254876)
(dschubert@sjk.law)
Amber L. Schubert (S.B.N. 278696)
(aschubert@sjk.law)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union. St., Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161

*Counsel for Plaintiffs Charles Byrd and
Vanessa Wilson and the Putative Class*

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO / OAKLAND DIVISION**

CHARLES BYRD and VANESSA WILSON,
Individually and on Behalf of All Others
Similarly Situated,

Plaintiffs,

v.

POSTMEDS, INC. d/b/a TRUEPILL,
Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Upon personal knowledge as to their own acts, and based upon their investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiffs Charles Byrd and Vanessa Wilson, on behalf of themselves and all others similarly situated, allege as follows:

SUMMARY OF THE ACTION

1. Plaintiffs bring this class action against Postmeds, Inc. d/b/a Truepill (“Postmeds”) for its failure to adequately secure and safeguard their and at least 2,364,359 other individuals’ personally identifying information (“PII”) and protected health information (“PHI”), including patient names, their medication type, demographic information, and prescribing physicians, among other potentially sensitive, private, and confidential data.

2. Postmeds is a digital pharmacy provider that fulfills mail-order prescriptions for customers of Folx, Hims, GoodRx, Cost Plus Drugs, and other online healthcare companies. It claims to have served more than three million total patients and delivered over twenty million prescriptions. Postmeds assures patients and customers that it “respects your privacy,” touting that it takes data security “very seriously and has established security standards and procedures to prevent unauthorized access to patient information.”¹

3. In the course of providing healthcare services to its customers and fulfilling prescription orders, individuals provided Postmeds (or Postmeds otherwise received) PII and PHI from millions of persons. In turn, Postmeds comes into the possession of, and maintains extensive files containing, the PII and PHI of its customers, patients, and other persons, and owes these individuals an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, Postmeds utilized deficient data security practices, thereby allowing millions of persons’ sensitive and private data to fall into the hands of strangers.

4. Between August 30, 2023 and September 1, 2023, Postmeds lost control over this highly sensitive and confidential PII and PHI of Plaintiffs and the Class Members (defined herein) in a massive and preventable data breach apparently perpetrated by cybercriminals (the “Data Breach”). According to Postmeds, on August 31, 2023, it detected that a “bad actor” had gained

¹ Privacy Policy, TRUEPILL, <https://www.truepill.com/legal/privacy> (last accessed Jan. 8, 2024).

1 remote access to a subset of its files used for pharmacy management and fulfilment services.
2 Postmeds then claims to have “immediately launched an investigation with assistance from
3 cybersecurity professionals and worked to quickly secure our environment.” Yet, according to
4 Postmeds’s own description of the events, the cybersecurity incident lasted at least one additional
5 day until September 1, 2023 before the bad actor’s access was cut off. Thus, cybercriminals had
6 unfettered access to Plaintiffs’ and the Class’s highly private information for three days.

7 5. The Data Breach was directly and proximately caused by Postmeds’s failure to
8 implement reasonable and industry-standard data security practices necessary to protect its systems
9 from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII
10 and PHI of almost 2.4 million individuals is now in the hands of cybercriminals, who target this
11 sensitive data for its value to identity thieves. Plaintiffs and Class Members are now at a significantly
12 increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks
13 which may last the rest of their lives. Consequently, Plaintiffs and Class Members must devote
14 substantially more time, money, and energy to protect themselves, to the extent possible, from these
15 crimes. Moreover, Plaintiffs and Class Members have lost the inherent value of their private data.

16 6. By aggregating information obtained from the Data Breach with other sources or
17 other methods, criminals can assemble a full dossier of private information on an individual to
18 facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims’ names and
19 other personal information to open new financial accounts, incur credit charges, obtain government
20 benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person
21 whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have
22 devastating consequences for the victim, causing years of often irreversible damage to their credit
23 scores, financial stability, and personal security. Likewise, the exfiltration of protected health
24 information puts Plaintiffs and the Class Members at a present and continuing risk of medical
25 identity theft, which poses an even more critical threat to victims because such fraud could lead to
26 loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring
27 substantial medical debt.
28

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

7. Despite the Data Breach being first detected on August 31, 2023, Postmeds only began notifying impacted persons *nearly two months later*, on October 30, 2023, exacerbating the damages and risks to Class Members, and in violation of various state data breach notification statutes. The data breach notice letters also obscure the true nature of the Postmeds cyberattack and threat it posed—failing to adequately inform Plaintiffs and Class Members how many people were impacted, how the “bad actor” accessed Postmeds’s systems and the root cause of the Data Breach, what “demographic information” was stolen, whether the exfiltrated information was encrypted or anonymized, why it took so long to notify victims, whether Postmeds notified law enforcement of the Data Breach, or what specific remedial steps Postmeds has taken to safeguard PII and PHI within its systems and networks (or otherwise purge unnecessary information) and to prevent further cyberattacks going forward. Without these critical details, Plaintiffs and Class Members cannot meaningfully mitigate the resulting effects of the Postmeds Data Breach.

8. Plaintiffs Byrd and Wilson are both Data Breach victims and first received a notification of the Data Breach from Postmeds by letters dated October 30, 2023.

9. Plaintiffs, on behalf of themselves and all others similarly situated, herein allege claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment or quasi-contract, invasion of privacy, violation of Texas’s Deceptive Trade Practices-Consumer Protection Act (TEX. BUS. & COM. CODE §§ 17.41, *et seq.*), violation of Maine’s Unfair Trade Practices Act (5 ME. REV. STAT. §§ 205-A, *et seq.*), violation of Maine’s Uniform Deceptive Trade Practices Act (10 ME. REV. STAT. §§ 1211, *et seq.*), and declaratory and injunctive relief. Plaintiffs, on behalf of themselves and the Class, seek: (i) actual damages, economic damages, statutory damages, and nominal damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendant’s custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for Postmeds to provide long-term identity theft protective services to Plaintiffs and Class Members; and (v) such other relief as the Court deems just and proper.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

PARTIES

A. Plaintiffs

10. Plaintiff Charles Byrd is a resident and citizen of Texas.

11. Plaintiff Vanessa Wilson is a resident and citizen of Maine.

B. Defendant

12. Defendant Postmeds, Inc. d/b/a Truepill is a Delaware corporation headquartered at 3121 Diablo Avenue, Hayward, California 94545.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the putative Class, as defined below, is a citizen of a state other than that of Defendant, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

14. This Court has general personal jurisdiction over Postmeds because it maintains its principal place of business in Hayward, California and regularly conducts business in California, and has sufficient minimum contacts in California, such as to not offend traditional notions of fair play and substantial justice.

15. Venue in this District is proper under 28 U.S.C. § 1391 because Postmeds resides in this District and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting or storing the PII and PHI of Plaintiffs and the putative Class Members.

16. Divisional Assignment: This action arises in Alameda County, in that a substantial part of the events which give rise to the claims asserted herein occurred in Alameda County, where Postmeds is headquartered and located. Pursuant to L.R. 3-2(d), all civil actions that arise in Alameda County shall be assigned to the San Francisco or Oakland Division.

FACTUAL BACKGROUND**A. Postmeds Collects, Stores, and Maintains Huge Amounts of Personally Identifiable Information and Protected Health Information.**

17. Postmeds, which does business as “Truepill,” was founded in 2016 and is a digital healthcare company specializing in pharmacy delivery services. It operates a wide network of mail order and specialty pharmacies, and fulfills prescriptions for popular online healthcare companies such as Folx, Hims, GoodRx, Cost Plus Drugs, and others. All told, Postmeds has served more than three million patients, delivering over twenty million total prescriptions to all fifty states.² It purports to “[d]eliver accessible and convenient care to every patient.”³

18. To utilize Postmeds’s pharmacy services, patients—like Plaintiffs Byrd and Wilson and Class Members—must provide their doctors, medical professionals, or Defendant directly with highly sensitive and private information.

19. Postmeds understands that data cybersecurity is critical. It “ensure[s]” healthcare partners that its technology “meets rigorous privacy and security standards.”⁴ Among the “Responsibilities” described in its Notice of HIPAA Privacy Practices, Postmeds admits it is “required by law to maintain the privacy and security of your protected health information” and promises to “let you know promptly if a breach occurs that may have compromised the privacy or security of your information.”⁵ Postmeds’s separate Privacy Policy goes a step further, declaring in bold type that “**Truepill respects your privacy.**”⁶ Elaborating, the policy explains that Postmeds is “committed” to protecting patient privacy, “takes the security of information very seriously,” and “has established security standards and procedures to prevent unauthorized access to patient information.”⁷

² <https://www.truepill.com/> (last accessed Jan. 8, 2024).

³ *Id.*

⁴ *Id.*

⁵ Notice of HIPAA Privacy Practices, TRUEPILL, <https://www.truepill.com/legal/nopp> (last accessed Jan. 8, 2024).

⁶ Privacy Policy, TRUEPILL, *supra* note 1.

⁷ *Id.*

20. Despite these strong proclaimed proactive policies and approaches to data security and privacy for its customers and healthcare partners, Postmeds failed to adequately secure and safeguard its systems and networks from a foreseeable and preventable cyberattack. This conduct proximately resulted in the Data Breach and significant harm to Plaintiffs and the Class.

B. The Postmeds Data Breach Exposed Valuable PII and PHI

21. Postmeds collected and maintained Plaintiffs' and the Class's PII and PHI in its computer systems, servers, and networks. In accepting, collecting, and maintaining Plaintiffs' and the Class's PII and PHI, Postmeds agreed that it would protect and safeguard that data by complying with state and federal laws and regulations and applicable industry standards. Postmeds was in possession of Plaintiffs' and the Class's PII and PHI before, during, and after the Data Breach.

22. According to Postmeds's Data Breach letters, Postmeds first detected that a "bad actor gained access to a subset of files used for pharmacy management and fulfillment services" on August 31, 2023.⁸ Following an investigation with assistance from cybersecurity experts, Postmeds determined that the Data Breach lasted for three days, between August 30, 2023 and September 1, 2023.⁹ Beginning on October 30, 2023—almost two months after the Data Breach occurred—Postmeds then reported the Data Breach to various governmental agencies and attorneys general.

23. Despite Postmeds's duties and commitments to safeguard sensitive and private information, Postmeds failed to follow industry-standard practices in securing Plaintiffs' and the Class Members' PII and PHI, as evidenced by the Data Breach.

24. In response to the Data Breach, Postmeds contends that it "worked quickly to secure our environment" and was "enhancing our security protocols and technical safeguards in response to this incident," as well as "increasing awareness of cybersecurity threats through additional employee training."¹⁰ Although Postmeds failed to expand on what these purportedly enhanced "security protocols and technical safeguards" are, such policies and practices clearly should have been in place and fully operational *before* the Data Breach. Nor do the Data Breach letters indicate

⁸ See Exhibit 1.

⁹ See *id.*

¹⁰ See *id.*

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

whether Postmeds notified law enforcement of the cybersecurity incident or whether the “bad actor” has been identified or apprehended.

25. As of October 30, 2023, Postmeds reported to the U.S. Department of Health and Human Services that the total number of persons affected by the Data Breach was 2,364,359.

26. Postmeds’s Data Breach letters reveal that the following information for Plaintiffs and the Class was stolen in the cyberattack: patient names, medication type, demographic information, and prescribing physician names.

27. Through its Data Breach notice letters to Plaintiffs and Class Members, Postmeds also recognized the actual imminent harm and injury that flowed from the Data Breach by encouraging them to “regularly review” their information for accuracy, including information they receive from healthcare providers.¹¹ The fraudulent activity resulting from the Data Breach may not come to light for years. Yet, Postmeds did not offer any compensation or complimentary credit monitoring or identity theft protection services to affected persons. Thus, the risk of identity theft and unauthorized use of Plaintiffs’ and Class Members’ PII and PHI remain very high.

C. The Healthcare Sector Is Increasingly Susceptible to Data Breaches, Giving Postmeds Ample Notice That It Was a Likely Cyberattack Target

28. At all relevant times, Defendant knew, or should have known, that the PII and PHI it was entrusted with was a target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals’ detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

29. As custodian of Plaintiffs’ and Class Members’ PII and PHI, Postmeds knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if any data breach occurred.

30. Postmeds was on notice that the FBI has been long concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning

¹¹ *See id.*

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

1 stated that “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for
 2 the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable
 3 Information (PII).”¹²

4 31. Defendant’s security obligations were especially important due to the substantial
 5 increase of cyberattacks and data breaches in recent years, particularly those targeting healthcare
 6 businesses and other organizations like Defendant, which store and maintain large volumes of PII
 7 and PHI. These largescale cyberattacks are increasingly common and well-publicized. Through the
 8 end of November 2023, 640 largescale cyberattacks had targeted hospitals, health systems, and
 9 healthcare records in 2023, affecting more than 115 million people—making 2023 the “worst-ever
 10 year for breached healthcare records.”¹³ With the surging number of such attacks targeting
 11 companies in the healthcare sector, Postmeds knew or should have known that it was at high risk of
 12 cyberattack and should have taken additional and stronger precautions and preemptive measures.

13 **D. Postmeds Breached Its Duties to Plaintiffs and the Class Members, and Failed**
 14 **to Comply with Regulatory Requirements and Industry Practices.**

15 32. Because Defendant was entrusted with PII and PHI at all times herein relevant,
 16 Postmeds owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and
 17 care in handling, using, maintaining, storing, and safeguarding the PII and PHI in its care, control,
 18 and custody, including by implementing industry-standard security procedures sufficient to
 19 reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred,
 20 and to promptly detect and thwart attempts at unauthorized access to its networks and systems.
 21 Defendant also owed a duty to safeguard PII and PHI because it was on notice that it was handling
 22 highly valuable data and knew there was a significant risk it would be targeted by cybercriminals.
 23 Furthermore, Postmeds knew of the extensive, foreseeable harm that would ensue for the victims of
 24 a data breach, and therefore also owed a duty to reasonably safeguard that information.

25
 26 ¹² Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20,
 27 2014), <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820>.

28 ¹³ November 2023 Healthcare Data Breach Report, THE HIPAA JOURNAL (Dec. 21, 2023), <https://www.hipaajournal.com/november-2023-healthcare-data-breach-report/>.

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

33. Security standards commonly accepted among businesses like Postmeds that store PII and PHI include, without limitation:

- i. Maintaining a secure firewall configuration;
- ii. Monitoring for suspicious or irregular traffic to servers or networks;
- iii. Monitoring for suspicious credentials used to access servers or networks;
- iv. Monitoring for suspicious or irregular activity by known users;
- v. Monitoring for suspicious or unknown users;
- vi. Monitoring for suspicious or irregular server requests;
- vii. Monitoring for server requests for PII or PHI;
- viii. Monitoring for server requests from VPNs; and
- ix. Monitoring for server requests for Tor exit nodes.

34. The U.S. Federal Trade Commission (“FTC”) publishes guides for businesses for cybersecurity¹⁴ and protection of PII which includes basic security standards applicable to all types of businesses.¹⁵

35. The FTC recommends that businesses:

- i. Identify all connections to the computers where sensitive information is stored.
- ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
- iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
- iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not

¹⁴ Start with Security: A Guide for Business, FTC (June 2015), *available at* <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

¹⁵ Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

1 necessary on a certain computer, a business should consider closing the ports to those services on
2 that computer to prevent unauthorized access to that machine.

3 v. Pay particular attention to the security of their web applications—the software
4 used to give information to visitors to their websites and to retrieve information from them. Web
5 applications may be particularly vulnerable to a variety of hacker attacks.

6 vi. Use a firewall to protect their computers from hacker attacks while it is
7 connected to a network, especially the internet.

8 vii. Determine whether a border firewall should be installed where the business's
9 network connects to the internet. A border firewall separates the network from the internet and may
10 prevent an attacker from gaining access to a computer on the network where sensitive information
11 is stored. Set access controls—settings that determine which devices and traffic get through the
12 firewall—to allow only trusted devices with a legitimate business need to access the network. Since
13 the protection a firewall provides is only as effective as its access controls, they should be reviewed
14 periodically.

15 viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an
16 eye out for activity from new users, multiple log-in attempts from unknown users or computers, and
17 higher-than-average traffic at unusual times of the day.

18 ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly
19 large amounts of data being transmitted from their system to an unknown user. If large amounts of
20 information are being transmitted from a business's network, the transmission should be investigated
21 to make sure it is authorized.

22 36. As described further below, Defendant owed a duty to safeguard PII and PHI under
23 several statutes, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") and
24 as a covered entity under the Health Insurance Portability and Accountability Act of 1996
25 ("HIPAA"), to ensure that all information it received, maintained, and stored was secure. These
26 statutes were enacted to protect Plaintiffs and the Class Members from the type of conduct in which
27 Defendant engaged, and the resulting harms Defendant proximately caused Plaintiffs and the Class
28 Members.

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

37. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiffs and Class Members. Under HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the PII and PHI of Plaintiffs and Class Members which was collected in conjunction with receiving medical services.

38. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of healthcare services to its clients and customers, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Member's confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Postmeds also violated its duties under the FTC Act and HIPAA.

39. Defendant failed to prevent the Data Breach. Had Postmeds properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

40. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII and PHI to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Postmeds further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members.

E. The Experiences of Plaintiffs Byrd and Wilson

41. Plaintiffs Byrd and Wilson both received notice of the Data Breach by letter from Postmeds dated October 30, 2023.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

42. As a proximate result of the Data Breach, Byrd and Wilson will spend time for the foreseeable future and beyond dealing with its consequences and self-monitoring their accounts and credit reports to monitor potentially suspicious and fraudulent activity. This time will be lost forever and cannot be recaptured. Following the Data Breach, Wilson has already experienced suspicious activity on her Venmo account in September 2023 wherein her password credentials were changed multiple times on the same day without her consent. Wilson spent several hours to resolve the incident, which temporarily suspended her Venmo account, and purchased security software.

43. In the months following the Data Breach, Byrd has experienced a significant uptick in phishing emails, texts, and phone calls, which he believes may have resulted from the Data Breach. Prior to the Data Breach, Byrd rarely received spam emails or spam texts, and spam phone calls were infrequent (one or two every four days). Now, Byrd is bombarded with spam emails (about twenty per day), around five daily spam phone calls, and multiple spam texts every week. In the months following the Data Breach, Wilson has also experienced an uptick in phishing texts and spam telephone calls (about two spam texts and two spam calls daily), which she believes resulted from the Data Breach.

44. Plaintiff Byrd has and is experiencing fear, stress, and frustration because his sensitive information was stolen in the Data Breach, and not knowing by whom or for what purpose. This goes beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

45. Byrd and Wilson suffered actual injuries in the form of damages to and diminution in the value of their PII and PHI—a form of intangible property was entrusted to Postmeds, which was compromised in and as a proximate result of the Data Breach.

46. Byrd and Wilson have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from their PII and PHI being obtained by unauthorized third parties and possibly cybercriminals.

47. Byrd and Wilson have a continuing interest in ensuring that their PII and PHI, which remains within Postmeds's possession and control, is protected and safeguarded against future data breaches or cybersecurity risks.

48. Defendant deprived Byrd and Wilson of the earliest opportunity to guard themselves against the Data Breach’s harmful effects by failing to promptly notify them about it. Instead, *Postmeds waited almost two months*, without any explanation whatsoever.

F. Plaintiffs Byrd and Wilson and the Class Suffered Actual and Impending Injuries Resulting From the Data Breach

49. As a proximate result of Defendant’s completely unreasonable security practices, identity thieves now possess the sensitive PII and PHI of Byrd, Wilson, and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Byrd, Wilson, and the Class. On the dark web—an underground Internet black market—criminals openly buy and sell stolen PII and PHI to create “identity kits” worth up to \$2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.¹⁶ And, “[t]he damage to affected [persons] may never be undone.”¹⁷

50. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals’ ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim’s identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an

¹⁶ Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, <https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d>.

¹⁷ *Id.*

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

identity theft victim was \$1,160 per person.¹⁸ Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.¹⁹

51. As a consequence of the Data Breach, Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

52. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.²⁰ The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to “pay an average of \$13,500 to resolve the crime.”²¹

53. Postmeds's data breach notices provide no compensation or relief whatsoever to affected persons for its wrongful conduct and actions described herein. Therein, Postmeds merely

¹⁸ Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* <https://bjs.ojp.gov/document/vit21.pdf>.

¹⁹ *Id.*

²⁰ Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FTC, *available at* <https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf> (last accessed Jan. 8, 2024).

²¹ Justin Klawans, *What is medical identity theft and how can you avoid it?*, THE WEEK (Aug. 2, 2023), <https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid>.

expresses “regret” for any “inconvenience or concern” it caused, which is completely inadequate under the circumstances. After a cybersecurity incident such as the one perpetrated here, the breached company typically offers years-long free identity protection services to affected individuals.

CLASS ACTION ALLEGATIONS

54. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the “Nationwide Class” or the “Class”):

All persons whose PII or PHI was compromised in the Data Breach discovered by Postmeds on or about August 31, 2023, including all persons who were sent a notice of the Data Breach (and each person a “Class Member”).

55. Within the Nationwide Class, there are two Subclasses defined as follows:

All persons residing in the State of Texas whose PII or PHI was compromised in the Data Breach discovered by Postmeds on or about August 31, 2023, including all Texas residents who were sent a notice of the Data Breach (the “Texas Subclass,” and each person a “Texas Subclass Member”).

All persons residing in the State of Maine whose PII or PHI was compromised in the Data Breach discovered by Postmeds on or about August 31, 2023, including all Maine residents who were sent a notice of the Data Breach (the “Maine Subclass,” and each person a “Maine Subclass Member”).

56. Excluded from the Nationwide Class and Subclasses are governmental entities, Postmeds, any entity in which Postmeds has a controlling interest, and Postmeds’s officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and Subclasses are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

57. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

58. Numerosity Under Rule 23(a)(1). The Nationwide Class and Subclasses are so numerous that the individual joinder of all members is impracticable, and the disposition of the

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

claims of all members of the Nationwide Class and Subclasses in a single action will provide substantial benefits to the parties and the Court. Although the precise number of members of the Nationwide Class and Subclasses are unknown to Plaintiffs at this time, on information and belief, the proposed Nationwide Class contains at least 2,364,359 individuals, as reported to the U.S. Department of Health and Human Services on October 30, 2023. On information and belief and given the size of the Nationwide Class, the proposed Subclasses contains at least thousands of individuals. Discovery will reveal, through Postmeds's records, the approximate number of members of the Nationwide Class and Subclasses.

59. Commonality Under Rule 23(a)(2). Common legal and factual questions exist that predominate over any questions affecting only individual members of the Nationwide Class and Subclasses. These common questions, which do not vary among members of the Nationwide Class or the Subclasses and which may be determined without reference to any Nationwide Class or Subclass Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

b. Whether Defendant failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that its computer systems and networks were protected;

c. Whether Defendant failed to take available steps to prevent and stop the Data Breach from occurring;

d. Whether Defendant owed a legal duty to Plaintiffs and Class Members to protect their PII and PHI;

e. Whether Defendant breached any duty to protect the PII or PHI of Plaintiffs and Class Members by failing to exercise due care in protecting their sensitive and private information;

f. Whether Defendant provided timely, accurate, and sufficient notice of the Data Breach to Plaintiffs and the Class Members;

g. Whether Plaintiffs and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

h. Whether Plaintiffs and Class Members are entitled to injunctive or equitable relief, including restitution.

60. Typicality Under Rule 23(a)(3). Plaintiffs' claims are typical of the claims of the Nationwide Class and Subclasses. Byrd and Wilson, like all proposed members of the Class and Subclasses, had their PII or PHI compromised in the Data Breach. Postmeds's uniformly unlawful course of conduct injured Byrd, Wilson, Class Members, and members of the Subclasses in the same wrongful acts and practices. Likewise, Byrd, Wilson, and other Class Members must prove the same facts in order to establish the same claims.

61. Adequacy of Representation Under Rule 23(a)(4). Byrd and Wilson are adequate representatives of the Nationwide Class and Subclasses because they are Nationwide Class Members, Byrd and Wilson are members of the Texas and Maine Subclasses, respectively, and their interests do not conflict with the interests of the Nationwide Class or Subclasses. Byrd and Wilson have retained counsel competent and experienced in complex litigation and consumer protection class action matters such as this action, and Byrd and Wilson and their counsel intend to vigorously prosecute this action for the Nationwide Class's and Subclasses' benefit and have the resources to do so. Byrd and Wilson and their counsel have no interests adverse to those of the other members of the Nationwide Class or Subclasses.

62. Predominance and Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Nationwide Class and Subclass Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Nationwide Class and Subclasses will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Postmeds's wrongful conduct. Even if each Nationwide Class and Subclass Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it

1 requires individual resolution of common legal and factual questions. By contrast, the class action
 2 device presents far fewer management difficulties and provides the benefit of a single adjudication,
 3 economies of scale, and comprehensive supervision by a single court.

4 63. As a result of the foregoing, class treatment under Fed. R. Civ. P. 23(b)(2) and (b)(3)
 5 is appropriate.

6 **FIRST CAUSE OF ACTION**

7 **Negligence**

8 ***(On Behalf of Plaintiffs and the Nationwide Class)***

9 64. Plaintiffs incorporate by reference and reallege paragraphs 1-53 as if fully set forth
 10 herein.

11 65. In the course of providing pharmaceutical fulfillment services to its clients and
 12 customers, Defendant solicited, gathered, and stored the PII and PHI of Plaintiffs and Class
 13 Members. Because Defendant was entrusted with such PII and PHI at all times herein relevant,
 14 Postmeds owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and
 15 care in handling, using, maintaining, storing, and safeguarding the PII and PHI in its care, control,
 16 and custody, including by implementing industry-standard security procedures sufficient to
 17 reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred,
 18 and to promptly detect and thwart attempts at unauthorized access to its networks and systems. This
 19 duty arose independently from any contract.

20 66. Defendant knew, or should have known, of the risks inherent in collecting and storing
 21 massive amounts of PII and PHI, including the importance of adequate data security and the high
 22 frequency of ransomware attacks and well-publicized data breaches both generally and the
 23 increasing rate of cybercriminals specifically targeting the healthcare industry, like Defendant.
 24 Postmeds owed a duty of care to Plaintiffs and Class Members because it was foreseeable that
 25 Postmeds's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art
 26 industry standards concerning data security would result in the compromise of that sensitive
 27 information. Defendant acted with wanton and reckless disregard for the security and confidentiality
 28 of Plaintiffs' and the Class's PII and PHI by failing to limit access to this information to unauthorized

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

1 third parties and by not properly supervising both the way the PII and PHI was stored, used, and
2 exchanged, and those in its employ responsible for such tasks.

3 67. Defendant owed to Plaintiffs and members of the Class a duty to notify them within
4 a reasonable timeframe of any breach to the security of their PII and PHI. Postmeds also owed a duty
5 to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and
6 circumstances of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to
7 take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk
8 of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

9 68. Defendant also had a common law duty to prevent foreseeable harm to others.
10 Defendant had full knowledge of the sensitivity and high value of the PII and PHI that it stored and
11 the types of foreseeable harm and injury-in-fact that Plaintiffs and Class Members could and would
12 suffer if that PII and PHI were wrongfully disclosed, leaked, accessed, or exfiltrated. Postmeds's
13 conduct created a foreseeable and unreasonable risk of harm to Plaintiffs and Class Members, who
14 were the foreseeable victims of Postmeds's inadequate data security practices.

15 69. Defendant violated its duty to implement and maintain reasonable security
16 procedures and practices, including through its failure to adequately restrict access to its pharmacy
17 management and fulfillment file systems that held millions of individuals' PII and PHI or encrypt or
18 anonymize such data. Postmeds's duty included, among other things, designing, maintaining, and
19 testing Postmeds's information security controls to ensure that PII and PHI in its possession was
20 adequately secured by, for example, encrypting or anonymizing sensitive personal information,
21 installing intrusion detection and deterrent systems and monitoring mechanisms, and using access
22 controls to limit access to sensitive data.

23 70. Postmeds's duty of care also arose by operation of statute, as follows:

24 a. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"),
25 Defendant had a duty to provide fair and adequate computer systems and data security practices to
26 safeguard the PII and PHI of Plaintiffs and Class Members; and

27 b. Pursuant to HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45
28 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the PII and PHI of

1 Plaintiffs and Class Members which was collected in conjunction with receiving healthcare services.
2 Additionally, the HIPPA Breach Notification Rule, 45 C.F.R. § 164.400-414, required Defendant to
3 provide notice of the Data Breach to each affected individual “without unreasonable delay and in no
4 case later than 60 days following discovery of the breach.”

5 71. These statutes—the FTC Act and HIPAA—were enacted to protect Plaintiffs and the
6 Class Members from the type of wrongful conduct in which Defendant engaged.

7 72. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs’ and
8 Class Members’ PII and PHI by failing to implement and maintain adequate data security measures
9 to safeguard Plaintiffs’ and Class Members’ sensitive personal information, failing to encrypt or
10 anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks
11 to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer
12 necessary for its provision of pharmaceutical services to its clients and customers, allowing
13 unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent)
14 unauthorized access to, and exfiltration of, Plaintiffs’ and Class Member’s confidential and private
15 information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data
16 security measures which deviated from standard industry best practices at the time of the Data
17 Breach. Through these actions, Postmeds also violated its duties under the FTC Act and HIPAA.

18 73. The law imposes an affirmative duty on Defendant to timely disclose the
19 unauthorized access and theft of PII and PHI to Plaintiffs and Class Members so that they can take
20 appropriate measures to mitigate damages, protect against adverse consequences, and thwart future
21 misuses of their private information. Postmeds further breached its duties by failing to provide
22 reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendant
23 actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-
24 fact of Plaintiffs and Class Members. Timely disclosure was necessary so that Plaintiffs and Class
25 Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery
26 services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit
27 reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public
28

1 records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover
2 from identity theft and other harms.

3 74. As recently as October 2021, Postmeds was valued at \$1.6 billion and earned
4 approximately \$200 million in revenue in 2020, and accordingly had the financial and personnel
5 resources necessary to prevent the Data Breach. Postmeds nevertheless failed to adopt reasonable
6 data security measures, in breach of the duties it owed to Plaintiffs and Class Members.

7 75. Plaintiffs and Class Members had no ability to protect their PII and PHI once it was
8 in Postmeds's possession and control. Postmeds was in an exclusive position to protect against the
9 harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

10 76. But for Defendant's breach of its duty to adequately protect Class Members' PII and
11 PHI, Class Members' PII and PHI would not have been stolen. As a result of Postmeds's negligence,
12 Plaintiffs and Class Members suffered and will continue to suffer the various types of damages
13 alleged herein. There is a temporal and close causal connection between Postmeds's failure to
14 implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs
15 and Class Members.

16 77. As a direct and traceable result of Defendant's negligence, Plaintiffs and the Class
17 have suffered or will suffer an increased and impending risk of fraud, identity theft, damages,
18 embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to
19 mitigate and remediate the effects of the Data Breach. These harms to Plaintiffs and the Class
20 include, without limitation: (i) loss of the opportunity to control how their personal information is
21 used; (ii) diminution in the value and use of their personal information entrusted to Defendant;
22 (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with
23 the prevention, detection, and recovery from identity theft and unauthorized use of financial
24 accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit
25 misuse, including increased costs to use credit, credit scores, credit reports, and assets;
26 (vi) unauthorized use of compromised personal information to open new financial and other
27 accounts; (vii) continued risk to their personal information, which remains in Defendant's possession
28 and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

measures to protect the personal information in its possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

78. Defendant's negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendant's care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

79. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

SECOND CAUSE OF ACTION

Negligence Per Se

(On Behalf of Plaintiffs and the Nationwide Class)

80. Plaintiffs incorporate by reference and reallege paragraphs 1-53 as if fully set forth herein.

81. Pursuant to the FTC Act, 15 U.S.C. § 45, Postmeds had a duty to maintain fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII and PHI.

82. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Postmeds's duty to protect Plaintiffs' and the Class Members' PII and PHI.

83. Pursuant to HIPPA, 42 U.S.C. §§ 1302, *et seq.*, Postmeds also owed Plaintiffs and Class Members a duty to provide adequate data security practices and to safeguard their PII and PHI.

84. Postmeds's duty to use reasonable care in protecting confidential and sensitive data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

85. Postmeds violated its duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable or adequate data security practices and measures to protect Plaintiffs' and the Class's PII and PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI that Postmeds collected and stored and the foreseeable consequences of a cybersecurity data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

86. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

87. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and Class Members, Plaintiffs and the Class Members would not have been injured.

88. The injuries and harms suffered by Plaintiffs and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Postmeds knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and the Class Members to suffer the foreseeable harms associated with the exposure of their PII and PHI.

89. Defendant's various violations and its failure to comply with the applicable laws and regulations referenced above constitutes negligence *per se*.

90. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII and PHI; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

91. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Postmeds's possession and is subject to further unauthorized

disclosures so long as Postmeds fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

THIRD CAUSE OF ACTION

Invasion of Privacy

(On Behalf of Plaintiffs and the Nationwide Class)

92. Plaintiffs incorporate by reference and reallege paragraphs 1-53 as if fully set forth herein.

93. Plaintiffs and Class Members have a legally protected privacy interest in their PII and PHI, which is and was collected, stored, and maintained by Postmeds, and they are entitled to the reasonable and adequate protection of their PII and PHI against foreseeable unauthorized access, as occurred with the Data Breach.

94. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII and PHI from unauthorized parties and that their private information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

95. Postmeds unlawfully invaded the privacy rights of Plaintiffs and Class Members by engaging in the wrongful conduct described above, including by failing to protect their PII and PHI by permitting unauthorized third parties to access, exfiltrate, and view this private information. Likewise, Postmeds further invaded the privacy rights of Plaintiffs and Class Members, and permitted cybercriminals to invade the privacy rights of Plaintiffs and Class Members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what PII and PHI had been accessed, exfiltrated, and viewed by unauthorized third parties.

96. This invasion of privacy resulted from Defendant's failure to properly secure and maintain Plaintiffs' and the Class Members' PII and PHI, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

97. Plaintiffs' and the Class Members' PII and PHI is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and the Class Members' PII and PHI, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

98. The disclosure of Plaintiffs' and the Class Members' PII and PHI to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

99. Postmeds's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and the Class Members' sensitive, PII and PHI is such that it would cause serious mental injury, shame, embarrassment, or humiliation to people of ordinary sensibilities.

100. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and the Class Members' PII and PHI was without their consent, and in violation of various statutes, regulations, and other laws.

101. As a result of the invasion of privacy caused by Defendant, Plaintiffs and the Class Members suffered and will continue to suffer damages and injuries as set forth herein.

102. Plaintiffs and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that the Court deems just and proper.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

103. Plaintiffs incorporate by reference and reallege paragraphs 1-53 as if fully set forth herein.

104. Through their course of conduct, Plaintiffs and the Class Members entered into implied contracts with Postmeds under which Postmeds agreed to safeguard and protect their confidential and private PII and PHI and to timely and accurately notify Plaintiffs and Class Members if their information had been breached and compromised.

105. Postmeds acquired, stored, and maintained the PII and PHI of Plaintiffs and the Class that it received either directly from them or that Postmeds received from its healthcare clients.

106. Plaintiffs and Class Members were required to provide, or authorize the transfer of, their private information and health information in order for Postmeds to provide its pharmaceutical

1 fulfillment services. Plaintiffs and Class Members paid money, or money was paid on their behalf,
2 to Postmeds in exchange for such services.

3 107. Postmeds solicited, offered, and invited Class Members to provide their private
4 information and health information as part of Postmeds's regular business practices. Plaintiffs and
5 Class Members accepted Postmeds's offers and provided their private information and health
6 information to Postmeds.

7 108. Postmeds accepted possession of Plaintiffs' and Class Members' PII and PHI for the
8 purpose of providing pharmaceutical fulfillment services to Plaintiffs and Class Members.

9 109. When Plaintiffs and Class Members paid money and provided their PII and PHI to
10 their healthcare providers, either directly or indirectly, in exchange for goods or services, they
11 entered into implied contracts with their healthcare providers and their business associates, including
12 Postmeds, and intended and understood that PII and PHI would be adequately safeguarded as part
13 of that service. Alternatively, Plaintiffs and Class Members are the intended third-party beneficiaries
14 of data protection agreements entered into between Postmeds and its healthcare provider clients.

15 110. Postmeds's implied promise of confidentiality to Plaintiffs and Class Members
16 includes consideration beyond those pre-existing general duties owed under the FTC Act, HIPAA,
17 or other state or federal regulations. The additional consideration included implied promises to take
18 adequate steps to comply with specific industry data security standards and FTC guidelines on data
19 security.

20 111. Postmeds's implied promises include but are not limited to: (a) taking steps to ensure
21 that any agents who are granted access to PII and PHI also protect the confidentiality of that data;
22 (b) taking steps to ensure that the information that is placed in the control of its agents is restricted
23 and limited to achieve an authorized medical purpose; (c) restricting access to qualified and trained
24 agents; (d) designing and implementing appropriate retention policies to protect the information
25 against criminal data breaches; (e) applying or requiring proper encryption; (f) multifactor
26 authentication for access; and (g) other steps to protect against foreseeable data breaches.

27 112. Postmeds's implied promises to safeguard Plaintiffs' and Class Members' PII and
28 PHI are evidenced by, *e.g.*, representations in Defendant's Privacy Policy and Notice of HIPAA

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

1 Privacy Practices described above. The mutual understanding and intent of Plaintiffs and Class
 2 Members on the one hand, and Postmeds on the other, is further demonstrated by their conduct and
 3 course of dealing.

4 113. Plaintiffs and the Class Members would not have entrusted their PII and PHI to
 5 Postmeds in the absence of such an implied contract. Had Postmeds disclosed to Plaintiffs and the
 6 Class (or their physicians and healthcare providers) that it did not have adequate computer systems
 7 and security practices to secure sensitive data, Plaintiffs and the other Class Members (or their
 8 physicians and healthcare providers) would not have provided their PII and PHI to Postmeds.

9 114. Postmeds recognized that Plaintiffs' and Class Members' PII and PHI is highly
 10 sensitive and must be protected, and that this protection was of material importance as part of the
 11 bargain to Plaintiffs and the other Class Members.

12 115. Plaintiffs and the Class Members fully and adequately performed their obligations
 13 under the implied contracts with Postmeds.

14 116. Postmeds breached the implied contracts it made with Plaintiffs and the Class
 15 Members by failing to take reasonable measures to safeguard their PII and PHI as described herein,
 16 as well as by failing to provide accurate, adequate, and timely notice to them that their PII and PHI
 17 was compromised as a result of the Data Breach.

18 117. As a direct and proximate result of Postmeds's wrongful conduct, Plaintiffs and the
 19 other Class Members suffered and will continue to suffer damages in an amount to be proven at trial,
 20 or alternatively, nominal damages. Plaintiffs and Class Members are also entitled to injunctive relief
 21 requiring Postmeds to strengthen its data security systems, submit to future audits of those systems,
 22 and provide adequate long-term credit monitoring and identity theft protection services to all persons
 23 affected by the Data Breach.

24 **FIFTH CAUSE OF ACTION**
 25 **Unjust Enrichment / Quasi-Contract**
 26 ***(On Behalf of Plaintiffs and the Nationwide Class)***

27 118. Plaintiffs incorporate by reference and reallege paragraphs 1-53 as if fully set forth
 28 herein.

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

119. A monetary benefit was directly and indirectly conferred upon Defendant through its receipt of Plaintiffs' and Class Members' PII and PHI, which Postmeds used to facilitate the provision of pharmaceutical fulfillment services. Postmeds appreciated or had knowledge of these benefits conferred upon it by Plaintiffs and the Class.

120. Under principles of equity and good conscience, Defendant should not be permitted to retain the full monetary value of the benefits because Postmeds failed to adequately protect Plaintiffs' and Class Members' PII and PHI.

121. Plaintiffs and the Class Members have no adequate remedy at law. Postmeds continues to retain their PII and PHI while exposing this sensitive and private information to a risk of future data breaches while in Defendant's possession. Defendant also continues to derive a financial benefit from using Plaintiffs' and Class Members' PII and PHI.

122. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and the Class Members have suffered various types of damages alleged herein.

123. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it because of its misconduct described herein and the Data Breach.

SIXTH CAUSE OF ACTION

Texas Deceptive Trade Practices-Consumer Protection Act, TEX. BUS. & COM. CODE §§ 17.41, *et seq.* (On Behalf of Plaintiff Byrd and the Texas Subclass)

124. Plaintiff Byrd incorporates by reference and realleges paragraphs 1-53 as if fully set forth herein.

125. Postmeds is a "person," as defined by TEX. BUS. & COM. CODE § 17.45(3).

126. Plaintiff Byrd and the Texas Subclass Members are "consumers," as defined by TEX. BUS. & COM. CODE § 17.45(4).

127. Postmeds advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by TEX. BUS. & COM. CODE § 17.45(6).

1 128. Postmeds engaged in false, misleading, or deceptive acts and practices, in violation
2 of TEX. BUS. & COM. CODE § 17.46(b), including by:

3 a. Representing that goods or services had approval, characteristics, uses, or
4 benefits that they did not have;

5 b. Representing that goods or services were of a particular standard, quality, or
6 grade, when they were of another;

7 c. Advertising goods or services with intent not to sell them as advertised; and

8 d. Failing to disclose information concerning goods or services which was
9 known at the time of transaction when such failure to disclose such information was intended to
10 induce consumers into transactions which the consumers would not have entered had the information
11 been disclosed.

12 129. Postmeds's false, misleading, and deceptive acts and practices include:

13 a. Failing to implement and maintain reasonable and adequate security and
14 privacy measures to protect Plaintiff Byrd's and the Texas Subclass Members' PII and PHI, which
15 was a direct and proximate cause of the Data Breach;

16 b. Failing to identify and remediate foreseeable security and privacy risks and
17 adequately improve security and privacy measures despite knowing the risk of cybersecurity
18 incidents, which was a direct and proximate cause of the Data Breach;

19 c. Failing to comply with common law and statutory duties pertaining to the
20 security and privacy of Plaintiff Byrd's and the Texas Subclass Members' PII and PHI, including
21 duties imposed by the FTC Act, HIPAA, and Texas's data security statute, TEX. BUS. & COM. CODE
22 § 521.052, which was a direct and proximate cause of the Data Breach;

23 d. Misrepresenting that it would protect the privacy and confidentiality of
24 Plaintiff Byrd's and Texas Subclass Members' PII and PHI, including by implementing and
25 maintaining reasonable and adequate data security measures;

26 e. Misrepresenting that it would comply with common law and statutory duties
27 pertaining to the security and privacy of Plaintiff Byrd's and the Texas Subclass Members' PII and
28

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

1 PHI, including duties imposed by the FTC Act, HIPAA, and Texas's data security statute, TEX. BUS.
2 & COM. CODE § 521.052;

3 f. Omitting, suppressing, or concealing the material fact that it did not
4 reasonably or adequately secure Plaintiff Byrd's and the Texas Subclass Members' PII and PHI; and

5 g. Omitting, suppressing, or concealing the material fact that it did not comply
6 with common law and statutory duties pertaining to the security and privacy of Plaintiff Byrd's and
7 the Texas Subclass Members' PII and PHI, including duties imposed by the FTC Act, HIPAA, and
8 Texas's data security statute, TEX. BUS. & COM. CODE § 521.052.

9 130. Postmeds intended to mislead Plaintiff Byrd and the Texas Subclass Members and
10 induce them to rely on its misrepresentations and omissions.

11 131. Postmeds's misrepresentations and omissions were material because they were likely
12 to deceive reasonable consumers about the adequacy of Postmeds's data security and ability to
13 protect the confidentiality of consumers' PII and PHI.

14 132. Had Postmeds disclosed to Plaintiff Byrd and the Texas Subclass Members that its
15 data systems and networks were not secure and, thus, vulnerable to attack, Postmeds would have
16 been unable to continue its business and would have been forced to adopt reasonable and adequate
17 data security measures and comply with the law.

18 133. Postmeds was entrusted with sensitive and valuable PII and PHI regarding millions
19 of consumers, including Plaintiff Byrd and the Texas Subclass. Postmeds accepted the responsibility
20 of protecting the confidential data while keeping the inadequate state of its security controls secret
21 from the public. Accordingly, Plaintiff Byrd and the Texas Subclass Members acted reasonably in
22 relying on Postmeds's misrepresentations and omissions, the truth of which they could not have
23 reasonably discovered.

24 134. Postmeds had a duty to disclose the above facts due to the circumstances of this case,
25 the sensitivity and extensive nature of the PII and PHI in its possession, and generally accepted
26 business standards. Such a duty is implied by law due to the nature of the relationship between
27 consumers, including Plaintiff Byrd and the Texas Subclass, and Postmeds because consumers are
28

1 unable to fully protect their interests with regard to their data, and placed trust and confidence in
2 Postmeds. Postmeds's duty also arose from its:

- 3 a. Possession of exclusive knowledge regarding the security of the data in its
4 systems;
- 5 b. Active concealment of the state of its security; and/or
- 6 c. Incomplete representations about the security and integrity of its data systems
7 and networks, while purposefully withholding materials facts from Plaintiff Byrd and the Texas
8 Subclass that contradicted these representations.

9 135. Postmeds engaged in unconscionable actions or conduct, in violation of TEX. BUS. &
10 COM. CODE § 17.50(a)(3). Postmeds engaged in acts or practices which, to consumers' detriment,
11 took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair
12 degree.

13 136. Consumers, including Plaintiff Byrd and the Texas Subclass Members, lacked
14 knowledge about the deficiencies in Postmeds's data security because this information was
15 exclusively known by Postmeds. Consumers also lacked the ability, experience, or capacity to secure
16 the PII and PHI in Postmeds's possession or to fully protect their interests with regard to their
17 sensitive and private data. Plaintiff Byrd and the Texas Subclass Members lack expertise in
18 information security matters and do not have access to Postmeds's systems or network in order to
19 evaluate its security controls. Postmeds took advantage of its special skill and access to PII and PHI
20 to hide its inability to protect the security and confidentiality of Plaintiff Byrd and the Texas Subclass
21 Members' PII and PHI.

22 137. Postmeds intended to take advantage of consumers' lack of knowledge, ability,
23 experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that
24 would result. The unfairness resulting from Postmeds's conduct is glaringly noticeable, flagrant,
25 complete, and unmitigated. The Data Breach, which resulted from Postmeds's unconscionable
26 business acts and practices, exposed Plaintiff Byrd and Texas Subclass Members to a wholly
27 unwarranted risk of safety of the PII and PHI and security of their identity and credit, and worked a
28

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

1 substantial hardship on consumers. Plaintiff Byrd and the Texas Subclass Members cannot mitigate
 2 this unfairness because they cannot undo the Data Breach.

3 138. Postmeds acted intentionally, knowingly, and maliciously to violate Texas's
 4 Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff Byrd's and
 5 the Texas Subclass Members' rights. As a direct and proximate result of Postmeds's unconscionable
 6 and deceptive acts and practices, Plaintiff Byrd and Texas Subclass Members have suffered and will
 7 continue to suffer injury, ascertainable losses of money or property, and non-monetary damages,
 8 including, but not limited to:

9 a. Fraud and identity theft;
 10 b. Time and expenses relating to monitoring their financial accounts for
 11 fraudulent or suspicious activity;
 12 c. An increased, imminent risk of fraud and identity theft;
 13 d. Loss of value of their PII and PHI;
 14 e. Overpayment for Postmeds's services;
 15 f. Loss of the value of access to their PII and PHI; and
 16 g. The value of identity protection and credit monitoring services made
 17 necessary by the Data Breach.

18 139. Postmeds's unconscionable and deceptive acts or practices were a producing cause
 19 of Plaintiff Byrd's and Texas Subclass Members' injuries, ascertainable losses, economic damages,
 20 and non-economic damages, including their mental anguish.

21 140. Postmeds's violations of the Texas Deceptive Trade Practices-Consumer Protection
 22 Act present a continuing risk to Plaintiff Byrd and the Texas Subclass Members, as well as the
 23 general public.

24 141. Plaintiff Byrd and the Texas Subclass seek all monetary and non-monetary relief
 25 allowed by law, including economic damages; damages for mental anguish; treble damages for each
 26 act committed intentionally or knowingly; Court costs; reasonable and necessary attorneys' fees;
 27 injunctive relief, and any other relief which the Court deems proper.
 28

SIXTH CAUSE OF ACTION**Maine Unfair Trade Practices Act, 5 ME. REV. STAT. §§ 205-A, *et seq.*
(On Behalf of Plaintiff Wilson and the Maine Subclass)**

142. Plaintiff Wilson incorporates by reference and realleges paragraphs 1-53 as if fully set forth herein.

143. Postmeds is a “person” as defined by 5 ME. REV. STAT. § 206(2).

144. Postmeds’s conduct as alleged herein related was in the course of “trade and commerce” as defined by 5 ME. REV. STAT. § 206(3).

145. Plaintiff Wilson and Maine Subclass Members purchased goods and/or services for personal, family, and/or household purposes.

146. Postmeds engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 ME. REV. STAT. § 207, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Wilson’s and Maine Subclass Members’ PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to reasonably identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Wilson’s and Maine Subclass Members’ PII and PHI, including duties imposed by the FTC Act, HIPAA, and Maine’s data security statute, 10 ME. REV. STAT. § 1348, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Wilson’s and Maine Subclass Members’ PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Wilson’s and Maine Subclass Members’ PII and

1 PHI, including duties imposed by the FTC Act, HIPAA, and Maine's data security statute, 10 ME.
2 REV. STAT. § 1348;

3 f. Failing to timely and adequately notify Plaintiff Wilson and the Maine
4 Subclass Members of the Data Breach;

5 g. Omitting, suppressing, and concealing the material fact that it did not
6 reasonably or adequately secure Plaintiff Wilson's and Maine Subclass members' PII and PHI; and

7 h. Omitting, suppressing, and concealing the material fact that it did not comply
8 with common law and statutory duties pertaining to the security and privacy of Plaintiff Wilson's
9 and Maine Subclass Members' PII and PHI, including duties imposed by the FTC Act, HIPAA, and
10 Maine's data security statute, 10 ME. REV. STAT. § 1348.

11 147. Postmeds's representations and omissions were material because they were likely to
12 deceive reasonable consumers about the adequacy of Postmeds's data security and ability to protect
13 the confidentiality of consumers' PII and PHI.

14 148. Had Postmeds disclosed to Plaintiff Wilson and Maine Subclass Members that its
15 data systems were not secure and, thus, vulnerable to attack, Postmeds would have been unable to
16 continue its business and it would have been forced to adopt reasonable data security measures and
17 comply with the law. Instead, Postmeds was trusted with sensitive and valuable PII and PHI
18 regarding millions of consumers, including Plaintiff Wilson the Maine Subclass. Postmeds accepted
19 the responsibility of being a steward of this data while keeping the inadequate state of its security
20 controls secret from the public. Accordingly, because Postmeds held itself out as maintaining secure
21 systems for collecting and managing PII and PHI data, Plaintiff Wilson and the Maine Subclass acted
22 reasonably in relying on Postmeds's misrepresentations and omissions, the truth of which they could
23 not have reasonably discovered.

24 149. As a direct and proximate result of Postmeds's unfair and deceptive acts and conduct,
25 Plaintiff Wilson and Maine Subclass Members have suffered and will continue to suffer injury,
26 ascertainable losses of money or property, and monetary and non-monetary damages, including from
27 fraud and identity theft; time and expenses related to monitoring their financial accounts for
28

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

1 fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their
 2 PII and PHI.

3 150. Pursuant to 5 Me. Rev. Stat. § 213(1-A), counsel for Plaintiff Wilson will serve
 4 Defendant with notice of these Maine Unfair Trade Practices Act violations by certified mail, return
 5 receipt requested.

6 151. On behalf of Maine Subclass Members, Plaintiff Wilson presently seeks restitution
 7 and injunctive relief in the form of an order enjoining Defendant from continuing to violate the
 8 Maine Unfair Trade Practices Act. Unless and until Postmeds is restrained by order of the Court, its
 9 wrongful conduct will continue to cause irreparable injury to Plaintiff Wilson and the Maine
 10 Subclass.

11 152. If Defendant fails to timely rectify or otherwise these Maine Unfair Trade Practices
 12 Act violations described herein, individually and on behalf of the Maine Subclass, Plaintiff Wilson
 13 reserves her right to amend this Class Action Complaint to seek damages and any other relief the
 14 Court deems proper as a result of Defendant's Maine Unfair Trade Practices Act violations pursuant
 15 to 5 ME. REV. STAT. § 213(1).

16 **SEVENTH CAUSE OF ACTION**

17 **Maine Uniform Deceptive Trade Practices Act, 10 ME. REV. STAT. § 1211, *et seq.*** 18 ***(On Behalf of Plaintiff Wilson and the Maine Subclass)***

19 153. Plaintiff Wilson incorporates by reference and realleges paragraphs 1-53 as if fully
 20 set forth herein.

21 154. Postmeds is a "person" as defined by 10 ME. REV. STAT. § 1211(5).

22 155. Postmeds advertised, offered, or sold goods or services in Maine and engaged in trade
 23 or commerce directly or indirectly affecting the people of Maine.

24 156. While in the course of its business, Postmeds engaged in deceptive trade practices by
 25 making false representations, including representations that it had adequate computer systems and
 26 data security practices to protect personal and private health information, when such systems and
 27 practices were inadequate, in violation of 10 ME. REV. STAT. §§ 1212(E), (G), (I), and (L).

28 157. Defendant knew or should have known that its computer systems and data security
 practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

1 Postmeds's representations and omissions were material because they were likely to deceive
 2 reasonable consumers about the adequacy of Postmeds's data security and ability to protect the
 3 confidentiality of consumers' PII and PHI.

4 158. Maine Subclass Members are likely to be damaged by Defendant's deceptive trade
 5 practices.

6 159. Plaintiff Wilson and the Maine Subclass seek all available and appropriate relief
 7 under 10 ME. REV. STAT. § 1213, including, but not limited to, injunctive relief and attorneys' fees.

8 **EIGHTH CAUSE OF ACTION**
 9 **Injunctive/Declaratory Relief**
 10 ***(On Behalf of Plaintiffs and the Nationwide Class)***

11 160. Plaintiffs incorporate by reference and reallege paragraphs 1-53 as if fully set forth
 12 herein.

13 161. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
 14 authorized to enter a judgment declaring the rights and legal relations of the parties and to grant
 15 further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious
 16 and violate the terms of the federal and state statutes described herein.

17 162. Defendant owes a duty of care to Plaintiffs and Class Members, which required
 18 Postmeds to adequately monitor and safeguard Plaintiffs' and Class Members' PII and PHI.

19 163. Defendant and its officers, directors, affiliates, legal representatives, employees, co-
 20 conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to
 21 Plaintiffs and Class Members.

22 164. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs'
 23 and Class Members' PII and PHI and whether Defendant is currently maintaining data security
 24 measures adequate to protect Plaintiffs and Class Members from further data breaches that
 25 compromise their PII and PHI. Plaintiffs allege that Defendant's data security measures remain
 26 inadequate. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the
 27 compromise of their PII and PHI and the risk remains that further compromises of their private
 28 information will occur in the future.

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

1 165. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter
2 a judgment declaring, among other things, the following:

3 a. Defendant owes a legal duty to adequately secure the PII and PHI of Plaintiffs
4 and the Class within its care, custody, and control under the common law, HIPAA, and Section 5 of
5 FTC Act;

6 b. Defendant breached its duty to Plaintiffs and the Class by allowing the Data
7 Breach to occur;

8 c. Defendant's existing data monitoring measures do not comply with its
9 obligations and duties of care to provide reasonable security procedures and practices that are
10 appropriate to protect the PII and PHI of Plaintiffs and the Class within Postmeds's custody, care,
11 and control; and

12 d. Defendant's ongoing breaches of said duties continue to cause harm to
13 Plaintiffs and the Class.

14 166. This Court should also issue corresponding prospective injunctive relief
15 requiring Defendant to employ adequate security protocols consistent with healthcare industry
16 standards to protect the PII and PHI of Plaintiffs and the Class within its custody, care, and control,
17 including the following:

18 a. Order Defendant to provide lifetime credit monitoring and identity theft
19 insurance and protection services to Plaintiffs and Class Members; and

20 b. Order that, to comply with Defendant's obligations and duties of care,
21 Postmeds must implement and maintain reasonable security and monitoring measures, including,
22 but not limited to:

23 a. Engaging third-party security auditors/penetration testers as well as
24 internal security personnel to conduct testing, including simulated attacks, penetration tests, and
25 audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to
26 promptly correct any problems or issues detected by such third-party security auditors;

27 ii. Encrypting and anonymizing the existing PII and PHI within its
28 servers, networks, and systems to the extent practicable, and purging all such information which is

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

no longer reasonably necessary for Defendant to provide adequate pharmaceutical fulfillment services to its clients and customers;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

167. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another Postmeds data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiffs and the Class for the serious risks of future harm.

168. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

169. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent Postmeds data breach or cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII and PHI would be further compromised.

SCHUBERT JONCKHEER & KOLBE LLP
 2001 Union St., Suite 200
 San Francisco, CA 94123
 (415) 788-4220

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

- A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class and Subclasses;
- B. Entering judgment for Plaintiffs, the Class, and the Subclasses;
- C. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiffs and the Class by implementing improved security controls;
- D. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;
- E. Award statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;
- F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;
- G. Awarding to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and
- I. Granting such further and other relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all claims so triable.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

1 Dated: January 11, 2024

SCHUBERT JONCKHEER & KOLBE LLP

2 /s/ Dustin L. Schubert

3 Dustin L. Schubert

4 Robert C. Schubert (S.B.N. 62684)

5 Dustin L. Schubert (S.B.N. 254876)

6 Amber L. Schubert (S.B.N. 278696)

SCHUBERT JONCKHEER & KOLBE LLP

2001 Union St., Suite 200

San Francisco, California 94123

Telephone: (415) 788-4220

Facsimile: (415) 788-0161

E-mail: rschubert@sjk.law

dschubert@sjk.law

aschubert@sjk.law

*Counsel for Plaintiffs Charles Byrd and Vanessa
Wilson and the Putative Class*

Exhibit 1

Postmeds, Inc.
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name1>>
<<Address>>
<<Address 2>>
<<City>>, <<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>,

Postmeds, Inc. is a pharmacy company that fulfills prescription orders. At Postmeds, we are committed to providing outstanding pharmacy services and protecting the information in our care. We recently identified and addressed a cybersecurity incident involving some of that information and wanted to share with you what happened and the steps we are taking in response.

What Happened: On August 31, 2023, we discovered that a bad actor gained access to a subset of files used for pharmacy management and fulfillment services. We immediately launched an investigation with assistance from cybersecurity professionals and worked quickly to secure our environment.

What Information was Involved: Our investigation determined that the bad actor accessed the files between August 30, 2023 to September 1, 2023. One or more of those files contained your name and prescription information. The information varied by individual, but may have included medication type, demographic information, and/or prescribing physician. Importantly, your Social Security number was **not** involved, as Postmeds does not receive this information.

What We Are Doing and What You Can Do in Response: We want you to know that we are taking this incident very seriously and regret any inconvenience or concern this may cause you. We are enhancing our security protocols and technical safeguards in response to this incident, and we are increasing awareness of cybersecurity threats through additional employee training. We also encourage you to regularly review your information for accuracy, as a best practice, including information you receive from your healthcare providers.

For more information: If you have additional questions about this incident, please call our dedicated, confidential call center at 1-855-457-9143, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Postmeds, Inc.